Privacidad e Intimidad en Internet

Título: Privacidad e Intimidad en Internet. **Target**: Alumnos de la ESO. **Asignatura**: Informática. **Autor**: Sergio Mahiques Benavent, Ingeniero Técnico en Infomática de Gestión por la Universidad Politécnica de Valencia, Profesor de Informática en Educación Secundaria Obligatoria.

El presente artículo nos proporcionara una serie de herramientas y consejos básicos para que nuestra "estancia" en Internet sea lo más placentera posible o por lo menos, con los mínimos sobresaltos, puesto que a estas alturas ya deberíamos saber que en Internet no hay privacidad y cuanto antes lo asimilemos más fácil será paliar, en la medida de lo posible, los efectos que esto nos pueda ocasionar, y es aquí donde se enmarca el presente articulo.

Todo lo expuesto a continuación no es más que aplicar el sentido común, tal y como lo aplicamos en nuestra vida cotidiana, pero que no aplicamos en todas aquellas cosas que hacemos en Internet, puesto que muchas veces no nos paramos a pensar que puedan tener efectos adversos para nosotros.

Con todo esto, para mejorar nuestra intimidad y privacidad en Internet, es aconsejable usar el sentido común y, en la medida de lo posible, seguir los siguientes puntos que se desarrollaran a continuación.

1. IDENTIDAD DIGITAL FALSA

Lo primero que debemos saber y entender es que tenemos una identidad en Internet (o identidad digital, que se forma a partir de todas las páginas Web, foros y redes sociales en las que estamos registrados, como facebook, Twitter, Linkedin,…), llegando incluso, en cierto modo, a formarse una reputación digital, de forma que, por ejemplo, si participamos activamente en un foro, en dicho foro podremos ser un usuario respetado o repudiado en función de nuestros mensajes.

Una vez que entendemos esto, debemos saber que la mayoría de las personas cometemos el error de solapar nuestra identidad real (aquella que tiene un DNI y una dirección postal) con nuestra identidad digital en Internet, es decir, cuando en una página Web nos piden nuestros datos personales, cometemos el error de introducir los verdaderos, de forma que así solapamos ambas identidades y muchas veces no podemos distinguir cuando algo es real o no, por ejemplo, si nos llega un correo electrónico a nuestro nombre diciendo que hemos ganado la lotería o heredado dinero de un familiar lejano es posible que dudemos si es real o no. Por ello, vamos a proporcionar una serie de consejos para mitigar los posibles inconvenientes que se puedan producir. Por cierto, si en realidad ganáramos la lotería, tened por bien seguro que nadie nos buscaría para dárnosla.

1.1. CREAR UNA IDENTIDAD DIGITAL FALSA

Lo primero que debemos hacer para proteger nuestra intimidad en Internet es crear una identidad digital falsa, con un nombre y unos apellidos falsos (incluso una fecha de nacimiento falsa) y esta será la que usaremos en todas aquellas redes sociales, páginas Web y foros cuando nos soliciten nuestros datos personales. Esto es debido a que hay robots (programas informáticos que se dedican a recopilar toda la información publica que hay en Internet sobre las personas para después venderla a empresas que la usan con fines comerciales) escaneando Internet en busca de datos para crear fichas de las personas y nada podemos hacer para que borren estos datos, puesto que la información que recopilan es pública, por ello lo mejor que podemos hacer es entorpecer a todo aquel que quiere sacar beneficio con nuestros datos.

La queja que surge inmediatamente frente a este postulado es clara, la gente piensa que si se cambia sus datos personales, sus amigos no podrán encontrarlos por ejemplo en facebook, nada más lejos de la realidad si alguien es realmente nuestro amigo, es tan fácil como decirle: "en facebook me llamo XXXXXX" y problema solucionado. El único inconveniente es que las personas con las que hemos perdido el contacto no nos podrán encontrar. Pensemos en la gente famosa, seguro que tienen un facebook o twitter real, para estar en contacto con sus amigos (no el que conocen sus fans), seguro que no usan su verdadero nombre, es mas probable que usen un apodo o nick que les gusta pero nada tiene que ver con su nombre.

Al crear nuestra identidad falsa evitamos que cuando alguien busque nuestro nombre en Google (o buscadores similares) pueda conocer toda nuestra vida en tan solo unos minutos, porque quiÉn no ha buscado su nombre alguna vez en Google y lo que es peor, cuando lo hacíamos deseábamos salir, porque en un momento dado se tenia la falsa creencia de que no éramos nadie si no salíamos en Google; pero con el tiempo se ha visto que es todo lo contrario, es mejor no salir en Google y así proteger nuestra intimidad. Esto parece algo exagerado pero mi sobrino de 9 años ya busca información sobre sus maestros en Internet y les envía solicitudes de amistad al facebook, esto se evitaría si sus maestros hubieran usado una identidad falsa en Internet.

Esta claro que habrá algunas entradas del buscador (enlaces a páginas Web que devuelve cuando hacemos una búsqueda) que no podremos controlar, como por ejemplo si salimos en el BOE, en el DOGV o alguna pagina oficial, pero lo que si tenemos que hacer es minimizar todas aquellas que dependan de nosotros, para así pasar lo más inadvertidos posible en Internet.

Finalmente, en lo que respecta al tema de la identidad falsa, también es importante usar una foto de perfil falsa, puesto que en la mayoría de las redes sociales la foto de perfil es pública, por ello es mejor usar como foto principal la foto de un animal doméstico, paisaje o personaje de cómic, y así evitamos que si alguien busca nuestra foto en Google salga inmediatamente nuestra imagen.

Todo lo expuesto en este párrafo puede parecer exagerado pero pensemos por un momento que una persona que conozca nuestro nombre, nuestro DNI, nuestro teléfono móvil y nuestro correo electrónico puede conocer toda nuestra vida con solo hacer búsquedas en Google de cada uno de los conceptos anteriores. Podéis hacer un experimento, coged el nombre de vuestra pareja o mejor amig@ y buscadlo en Internet (nombre, teléfono, DNI, email) seguro que descubrís algo que no sabias (no tiene porque ser algo malo).

1.2. BORRAR FOTOS INAPROPIADAS

Al igual que no colgaríamos una foto nuestra en el balcón de nuestra casa en bikini o bañador, muchas veces sí que lo hacemos en las redes sociales. Esto que puede parecer lo más inocente del mundo, tiene el inconveniente de que nunca podremos controlar quién tiene nuestras fotos, por ello lo mejor es borrarlas y no subir fotos políticamente incorrectas.

Hay algunas redes sociales como Tuenti que permiten inhabilitar la opción de guardar fotos, es decir, nosotros podemos decidir si nuestros amigos se pueden bajar (guardar en su disco duro) o no la foto, pero debemos recordar que todo aquello que se muestra por pantalla se puede capturar simplemente pulsando la tecla "Imprimir pantalla" (tecla que al ser pulsada guarda el contenido de la pantalla en el portapapeles en formato imagen) y una vez capturada la pantalla, ya podemos editarla o guardarla.

Resumiendo, en este caso la mejor medicina es la prevención, si evitamos colgar fotos inapropiadas evitaremos que caigan en malas manos.

1.3. BORRAR GENTE QUE NO CONOCEMOS FISICAMENTE

Debemos ser muy cuidadosos con nuestros ciberamigos, puesto que actualmente mediante la ingeniería social (que consiste engañarnos para que nosotros proporcionemos nuestras contraseñas mediante el uso de paginas Web falsas) nos pueden sacar información sin darnos cuenta, simplemente a partir de la información de nuestras redes sociales pueden sacarnos una primera información que usen después en nuestra contra, es por esto que no debemos confiar en quienes no conocemos, puesto que desconocemos sus intenciones.

Pongamos el ejemplo de una persona que es un hincha del Real Madrid, alguien podría usar esta información para mandarle un correo electrónico diciendo que ha ganado una entrada para ver un partido y lo único que tiene que hacer es pinchar en un enlace y registrarse. Simplemente al registrarse ya esta proporcionando datos personales o, en el peor de los casos, podría estar siendo infectado por un virus sin siquiera esperarlo.

2. USO ADECUADO DEL CORREO ELECTRÓNICO

En lo referente al uso del correo electrónico hay una serie de conceptos que debemos tener claros para proteger nuestra privacidad y la de nuestros contactos. Así veremos que hay que usar más de un correo electrónico y usarlos adecuadamente.

2.1. MÍNIMO 3 CORREOS ELECTRÓNICOS

Otra buena idea para protegernos es tener un mínimo de 3 correos electrónicos, esto, a parte de ser una medida de protección, también nos sirve de primer filtro para separar nuestra vida personal y laboral. La idea es simple, hay que tener como mínimo un correo personal, un correo para el trabajo y un correo basura que usaremos para registrarnos en Webs, foros y redes sociales (el que usaremos con nuestra identidad digital falsa).

Puede parecer nuevamente excesivo, pero como ejemplo decir que en Estados Unidos una persona estaba de baja por depresión, su empresa harta de pagar la baja laboral pidió pruebas de si realmente estaba de depresión y simplemente tuvieron que entrar en el facebook del trabajador y comprobar que en realidad no estaba deprimido puesto que estaba continuamente de fiesta, como así se podía observar en las fotos que colgaba en la red, por este motivo es también una buena idea separar el mundo laboral del personal (y no tener a nuestro jefe agregado en el facebook).

Volviendo al tema de la identidad digital, si usamos 3 correos electrónicos también evitamos que cuando alguien un poco más experto busque nuestro correo electrónico (el que usamos en el trabajo o a nivel personal) lo pueda encontrar en algún foro o página Web, es decir, que nos pueden encontrar bien por nuestro nombre o bien por nuestro correo electrónico, pero si usamos distintos correos electrónicos para distintas cosas aumentamos nuestra privacidad (puesto que es raro que alguien conozca todos los correos electrónicos que usamos).

Nuevamente, si pensáis que es una tontería, haced la prueba y buscad vuestro correo electrónico (o incluso teléfono móvil), seguramente lo encontrareis en alguna página, foro, comentario o anuncio que no recordabais. Y en última instancia, seguro que a nadie le gustaría que alguien (como pueda ser nuestra pareja o vuestro jefe) encontrase vuestro correo electrónico o teléfono móvil en un anuncio “inapropiado” de Internet.

2.2. USAR EL CAMPO “CCO” DEL CORREO ELECTRÓNICO

En realidad así no nos protegemos nosotros, sino más bien, protegemos a todos nuestros contactos, eso sí, les pediremos que ellos hagan lo mismo, por ello siempre que vayamos a enviar un correo electrónico a más de un destinatario es conveniente usar el campo “cco” (con copia oculta) para así ayudar a proteger la intimidad de nuestros contactos.

El campo “cco” lo que hace es mandar un correo a todos los destinatarios que ahí escribimos pero con la salvedad de que nadie puede saber a quien más se le ha mandado ese correo. Pensemos por un momento en los inicios de Internet y los correos cadena, donde la gente reenviaba correos, y nos llegaban correos donde aparecían una infinidad de direcciones de gente que no conocíamos, para evitar esto debemos usar el campo “cco” y así el email de nuestros contactos permanece en el anonimato.